CLAIMS

We claim:

1. A method for ensuring the integrity of data, comprising:

for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating a cryptographic checksum for said plurality of said first data segments; and

enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

2. The method described in Claim 1 further comprising:

calculating a cryptographic checksum for said plurality of said second data segments; and

enabling said cryptographic checksum for said plurality of said second data segments to be transmitted separately from said plurality of data packets.

3. The method described in Claim 2 further comprising:

including said first cryptographic checksum for said plurality of said first data segments and said cryptographic checksum for said plurality of said second data segments in the same data packet.

4. The method described in Claim 1 wherein said cryptographic checksum for said plurality of said first data segments is calculated at a rate which is different from the rate at which said cryptographic checksum for said plurality of said second data segments is calculated.

5. The method described in Claim 1 wherein said calculating of said cryptographic checksum utilizes an opportunistic integrity checking scheme.

6. The method described in Claim 1 wherein said calculating of said cryptographic checksum is performed using a technique selected from the group consisting of:

a hash function providing a fingerprint of data contained in an encrypted data packet and which guarantees the authenticity of received data and the validity of decrypted data, Message Authentication Codes (MAC), Message Digest algorithms, keyed hashes, SHA (Secure Hash Algorithm), RIPEMD (RACE Integrity Primitives Evaluation Message Digest), HMAC (keyed-Hashing for Message Authentication), and digital signature schemes.

7. The method described in Claim 1 wherein said plurality of said data packets comprises secure scalably streamable data.

8. The method described in Claim 1 wherein said plurality of said data packets include data comprising scalably compressed data for media selected from the group consisting of:

speech, audio, image, video, and computer graphics.

9. The method described in Claim 1 wherein said plurality of said data packets include data scalably formatted according to techniques selected from the group consisting of:

JPEG-2000 with spatial, frequency, SNR (amplitude), region of interest, or color plane scalability; MPEG-1/2/4 or H.261/2/3/4 using spatial, temporal, or SNR (amplitude), region of interest (ROI) or object scalability or fine-grain scalability (FGS); scalable advanced audio coding (scalable AAC); object-based audio coding using MPEG-4 synthetic audio for individual compression and composition of multiple audio objects; and progressive/scalable graphics compression.

10. The method described in Claim 1 wherein said plurality of said data packets comprises media data.

11. The method described in Claim 1 wherein said data is stored in a storage medium.

12. The method described in Claim 1 further comprising:

encrypting one or more of said data packets.

13. The method described in Claim 1 further comprising:

encrypting said cryptographic checksum.

14. A computer readable medium having instructions stored therein for implementing a method for ensuring integrity of data, comprising:

for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating a cryptographic checksum for said plurality of said first data segments; and

enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of said data packets.

15. The computer readable medium described in Claim 14 wherein said instructions further comprise:

calculating a cryptographic checksum for said plurality of said second data segments; and

enabling said cryptographic checksum for said plurality of said second data segments to be transmitted separately from said plurality of said data packets.

16. The computer readable medium described in Claim 15 wherein said instructions further comprise:

including said first cryptographic checksum for said plurality of said first data segments and said cryptographic checksum for said plurality of said second data segments in the same data packet.

17. The computer readable medium described in Claim 14 wherein said cryptographic checksum for said plurality of said first data segments is calculated at a rate which is different from the rate at

which said cryptographic checksum for said plurality of said second data segments is calculated.

18. The computer readable medium described in Claim 14 wherein said data packets comprise secure scalably streamable data.

19. The computer readable medium described in Claim 14 wherein said data packets comprise media data.

20. The computer readable medium described in Claim 14 wherein said data is stored in a storage medium.

21. The computer readable medium described in Claim 14 wherein said instructions further comprise:

encrypting one or more of said data packets.

22. The computer readable medium described in Claim 14 wherein said instructions further comprise:

encrypting said cryptographic checksum.

23. An apparatus for ensuring integrity of data, comprising:

a receiver for receiving a plurality of data packets each of said packets comprising one or more data segments;

a cryptographic checksum calculator coupled to said receiver, said cryptographic checksum calculator for calculating a cryptographic checksum for one or more of said data segments; and a cryptographic checksum appender coupled to said cryptographic checksum calculator for assembling said cryptographic checksum.

24. The apparatus described in Claim 23 wherein said cryptographic checksum calculator is enabled to,

for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculate a cryptographic checksum for said plurality of said first data segments; and

to enable said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

25. The apparatus described in Claim 24 wherein said cryptographic checksum calculator is enabled to calculate said cryptographic checksum for said set of said data segments independently of cryptographic checksums calculated for other sets of said data segments.

26. The apparatus described in Claim 23, further comprising a forwarder for forwarding said packets to a destination.

27. A method for ensuring integrity of data, comprising:

receiving a data packet comprising an amount of data partitioned into a plurality of data segments;

calculating a cryptographic checksum for a first of said plurality of data segments; and

enabling said cryptographic checksum for said first of said plurality of data segments to be transmitted separately from said data packet.

28. The method described in Claim 27 further comprising:

calculating a second cryptographic checksum, wherein a second cryptographic checksum is computed for a second of said plurality of data segments, said first segment, and said cryptographic checksum for said first of said plurality of data segments.

29. A method for ensuring integrity of data, comprising:

receiving a data packet comprising an amount of data partitioned into at least one data segment;

calculating a cryptographic checksum for said at least one data segment; and

enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet.

30. The method described in Claim 29 further comprising:

calculating a second cryptographic checksum for a second of said at least one data segment; and enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet.

31. The method described in Claim 29 wherein said first cryptographic checksum and said second cryptographic checksum are transmitted in a common data packet.

32. An apparatus for verifying the integrity of data, said apparatus comprising:

a receiver, said receiver configured to receive data and a previously determined cryptographic checksum corresponding to said data; and

an integrity check module coupled to said receiver, said integrity check module configured to calculate a new cryptographic checksum corresponding to said received data and to determine whether said new cryptographic checksum matches said previously determined cryptographic checksum.

33. The apparatus of Claim 32 wherein said integrity check module is integral with said receiver.

34. The apparatus of Claim 32 further comprising:

an output coupled to said integrity check module, said output configured to provide an indication of whether said new cryptographic checksum matches said previously determined cryptographic checksum.